51. IWK

Internationales Wissenschaftliches Kolloquium
International Scientific Colloquium

PROCEEDINGS 11-15 September 2006

FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION SCIENCE

INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING - DEVICES AND SYSTEMS, MATERIALS AND TECHNOLOGIES FOR THE FUTURE

Startseite / Index:
http://www.db-thueringen.de/servlets/DocumentServlet?id=12391

TECHNISCHE UNIVERSITÄT
ILMENAU

Impressum

Herausgeber: Der Rektor der Technischen Universität Ilmenau
Univ.-Prof. Dr. rer. nat. habil. Peter Scharff

Redaktion: Referat Marketing und Studentische Angelegenheiten
Andrea Schneider

Fakultät für Elektrotechnik und Informationstechnik
Susanne Jakob
Dipl.-Ing. Helge Drumm

Redaktionsschluss: 07. Juli 2006

Technische Realisierung (CD-Rom-Ausgabe):
Institut für Medientechnik an der TU Ilmenau
Dipl.-Ing. Christian Weigel
Dipl.-Ing. Marco Albrecht
Dipl.-Ing. Helge Drumm

Technische Realisierung (Online-Ausgabe):
Universitätsbibliothek Ilmenau
ilmedia
Postfach 10 05 65
98684 Ilmenau

Verlag:
Verlag ISLE, Betriebsstätte des ISLE e.V.
Werner-von-Siemens-Str. 16
98693 Ilrnenau

ISBN (Druckausgabe): 3-938843-15-2
ISBN (CD-Rom-Ausgabe): 3-938843-16-0

Startseite / Index:
http://www.db-thueringen.de/servlets/DocumentServlet?id=12391

121251st Internationales Wissenschaftliches Kolloquium
Technische Universität Ilmenau
September 11 – 15, 2006

A. Yousef, A. Mitschele-Thiel, R. Boeringer, A. Diab

A New Framework to Support Mobility in Multi-hop Hybrid Networks

ABSTRACT

Connecting wireless devices to the Internet is of major interest in today's research. It is well known that the **W**ireless **L**ocal **A**rea **N**etwork (WLAN) standard will play a major role in the future communication networks. WLAN can be deployed in infrastructure or infrastructure-less mode, referred to as Ad hoc. WLAN offers high bit rate services. However, it is difficult to avoid not covered areas. To overcome this, a **M**obile **H**ost (MH) could use an intermediate MH as a relay to the **A**ccess **P**oint (AP). This leads to the so called hybrid multi-hops network structure, which can be created by enabling mobility support between infrastructure and infrastructure-less networks when the MH moves from an Ad hoc network connected to one AP to another which is connected to another one. In order to achieve this, new adequate solutions for inter-connecting infrastructure-based networks and Ad hoc networks should be developed. Throughout this paper, we propose a new solution to achieve a fast handoff in multi-hop hybrid networks. We extend the **A**d hoc **O**n-**D**emand Distance **V**ector routing protocol AODV to use the principle of fast authentication as it is described in **M**obile **I**P **F**ast **A**uthentication Protocol (MIFA), in such a way that the MH that moves from one network to another can still obtain Internet connectivity. Our solution should outperform the other solution with respect to the handoff latency. The MN can fast resume receiving and transmitting of data.

I- INTRODUCTION

The wireless communication networks are developed rapidly, the number of wireless devices such as portable or handheld computers, PDAs and cell phones increases drastically. Without Internet access for these devices their use will be limited so that

connecting wireless devices is of major interest in today's research. It is well known that the WLAN is a widely deployed standard [1] which enables wireless devices in infrastructure mode to communicate directly within one hop with the AP, which has access to Internet by its protocols such as MIP. This AP typically has both a wired and a wireless interface, and hence serves as a gateway between the two accesses media. WLAN standard can be deployed in infrastructure or infrastructure-less mode, referred to as Ad hoc [2]. An Ad hoc network is an autonomous system of mobile routers, the mobile ones connect to each other through multi-hops making the network scalable without limitation. WLAN offers high bit rate services. However, it is difficult to avoid not covered areas due to limitation of AP rang, dead zones or transmission phenomena such as multipath, fading and obstacles. As users want to maintain open connections with each other in Internet while not being restricted to certain physical areas, they will need the benefit of roaming between different networks. WLAN and Ad hoc alone cannot provide this requirements because WLAN has a restricted area with access to Internet and Ad hoc is unlimited without access to Internet so they should be integrated to offer advantages of the both.

However, the difficulty with roaming is that the protocols to manage the nods mobility in WLAN and Ad hoc are different. **M**obile **IP** (MIP) [3] protocol in WLAN allows mobile nodes that are away from their home network to register with a foreign agent and obtain a **C**are-**o**f **A**ddress (CoA) on the visited foreign network. The MH will be within direct transmission range of a foreign agent FA in order to register with this foreign agent, to obtain a CoA, and to acquire Internet connectivity. In Ad hoc the **A**d hoc **O**n-**D**emand Distance **V**ector routing protocol (AODV) [4] has been designed as a router protocol to discover and maintain multi-hop paths when MH moves within an Ad hoc network. AODV is a reactive routing protocol, meaning that route between source and destination is only discovered when source MH needs to connect. Once routes are discovered, they are maintained as long as needed by the source node.

In this paper we propose a solution to enable Internet connectivity of MHs within Ad hoc network through WLAN access point when one or more of them are located within the range of it and to maintain this connection when the MH move from this Ad hoc network to another which connects to another AP.

In this solution, we extend AODV to use the fast authentication principle used in **M**obile **I**P **F**ast **A**uthentication Protocol (MIFA) [5]. When the MH wants to connect to a **C**orresponding **N**ode (CN), which may be a node in the Ad hoc or in the Internet, it

tries to find a route to this CN in Ad hoc network. At the same time, it searches for the nearest Access Point (AP) that can connect the MH to the Internet. The MH connects with the AP through multi-hops and uses the MIP protocol to register itself with its Home Agent (HA) through the serving **F**oreign **A**gent (FA), if the CN is not in the Ad hoc network.

The remainder of this paper is organized as follows. Section II presents related work in the area of integrating Ad hoc network and WLAN. Then, section III provides an overview of Mobile IP, AODV and MIFA protocols. Section IV describes our solution fast handoff between Ad hoc and WLAN. Finally, section V concludes the paper.

II- RELATED WORKS

Several proposals for Internet connectivity and mobility management between wired IP networks and Ad hoc networks have been published. In [6] an approach describes how to connect a wired IP network running the protocol MIP with Ad hoc networks running the AODV. MIP is extended to operate in Ad hoc networks where MIP messages are managed by multiple hops instead of one hop as in the current specification of MIP, which enables MH multiple hops in the Ad hoc network from a FA to register. The AODV protocol is modified to create routes based on MIP messages to enhance performance. In [7] a scheme is introduced to develop a new integrated solution for IPv6-based hybrid multi-hop network by using Cellular IP (CIP) in the IP core and AODV in Ad hoc networks. The connectivity is achieved by extending the practical way of using a Co-located Care-of-address in CIPv6 to the Ad hoc network, thereby providing a way to preserve independent addressing. The integration is based on host routes. However, CIPv6 provides a promising basis for releasing efficient handoffs for distant mobile hosts.

The work [8] proposes that the foreign agent acts as gateway for Ad hoc network. When FA receives the route request from the MH it tries to inform the MH about the possible place of CN, if it is in Ad hoc network or in Internet. The reply message helps the MH to use the FA to connect to Internet. Before using the FA the MH must make sure that the CH is not within the Ad hoc network. For this, multiple route

requests are sent according to the maximum number of attempts configured. If no reply is received from the CH the FA will be used.

A gateway to interconnect Ad hoc networks and wired IP networks is presented in [9]. It extends MIP to manage multi-homing where network layer characteristics are used to decide the care-of address. This enhances a good handoff where the multi-homed MIP enables MHs in Ad hoc network to simultaneously connect to multiple gateways in different network. The same home address can be used as the final destination for all care-of addresses used by a MH.

Agent advertisements and agent solicitation are used in [10] to enable the MHs in Ad hoc networks to connect to Internet through gateway. AODV is used as the routing protocol in the Ad hoc network and MIP is used to manage mobility between gateways. By expanding route request message to piggyback the solicitations it will avoid the flooding. Intermediate nodes, receiving such a message, will respond with their gateway information so a route from MH to gateway will be created.

However, in the previous solutions the latency required to resume the session is too large and does not match the requirements of real-time application.

Therefore, it is necessary to develop new solutions to support seamless mobility in hybrid multi-hops networks.

III- OVERVIW OF MOBILE IP, AODV AND MIFA

3.1 MOBILE IP

Mobile IP protocol aims to provide continuous connectivity to a MH when it moves within different networks by providing transparent routing of IP datagrams. The maintenance of connections by taking care of routing is the main objective.

The basic entities constituting a MIP aware network are:

- Mobile Node (MN): A mobile user that changes his point of attachment from one network or sub-network to another.
- Home Agent (HA): A router in a home network, which maintains location information for the MN and tunnels the packets to the MN while it is away from its home network.

- Foreign Agent: A router in the mobile MN's visited (foreign) network. The foreign agent cooperates with the MN's home agent to deliver packets to the MN.
- Corresponding Node (CN): is another IP entity e.g. a host with which the MN communicates.

MIP introduces two separate IP addresses for MN as Home address and CoA. Each mobile node has a unique Home address and it should continue to use it to receive data, even when it leaves its home network. Every time while roaming a foreign network, however, the MN gets a CoA from FA in order to maintain existing sessions. This address provides information about the MN's current point of attachment to the Internet.

There are two methods to obtain the address:

- HAs and FAs periodically broadcast Agent Advertisements (Agnt_Adv) to advertise their presence.
- Optionally, MNs can send an Agent Solicitation (Agnt_sol) message to determine whether any prospective agents are present in the network.

A MN utilizes Agnt_Adv messages to determine whether it is in its home or foreign network. When a MN learns of the FA's presence, it selects a CoA in the foreign network from one of the advertised CoA in the Agnt_Adv.

Whereas MN is known by their home address from CN there is also the problem of using another address (CoA), so that to receive data packets on the foreign network, the mobile node must register its current care-of address with its home agent. A Registration Request (Reg_Rqst) message is transmitted by the MN to the HA through the FA. Upon the reception of the Reg_Rqst, the HA records the CoA of the MN and sends a Registration Reply (Reg_Rply) back to the MN, thereby acknowledging a successful registration.

Data packets, sent to the mobile node's home address, are intercepted by its home agent. The home agent tunnels those packets to the mobile node's care-of address. The Foreign agent decapsulates and forwards it to the mobile node.

3.2 AODV

The **A**d hoc **O**n-Demand **D**istance **V**ector (AODV) routing protocol aims to maintain the connectivity between the nodes when they move in Ad hoc network.

The main features of this protocol are:

- AODV is a reactive protocol that means it discovers the route when source node needs to communicate.
- It uses multi-hop mechanism to pass messages through their neighbours to nodes with which they cannot directly communicate.
- Nodes that do not lie on active paths maintain neither any routing information nor participate in any periodic routing table exchanges.
- AODV makes sure that these routes do not contain loops and tries to find the shortest possible route by utilizing per-node sequence numbers.
- AODV is also able to handle changes in routes and can create new routes when there is an error in the established route.

The AODV's missions consist of three steeps:

3.2.1 Path Discovery

Route discovery begins when a source node needs a route to a destination node.

It broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source (IP address, sequence number), the destination (IP address, sequence number), the lifespan of the message and a Broadcast- ID.

When a neighbouring MN receives the RREQ, it first creates a reverse route entry for the source node in its route table. It then checks whether it has an unexpired route to the destination node. In order to respond to the RREQ, the node must either be the destination itself, or it must have an unexpired route to the destination whose corresponding sequence number is at least as high as the one contained in the RREQ. If none of these conditions is met, the node rebroadcasts the RREQ. On the other hand, if one of these conditions is met, the node then creates a Route Reply (RREP) message. It places the current sequence number of the destination, as well as its distance in hops to the destination, into the RREP, and then unicasts this message back to the source. Intermediate nodes along the path to the source node create a forward route entry for the destination node in their route table. Once the source node receives the RREP, it can begin using the route to transmit data packets to the destination.

If the source node does not receive a RREP before its discovery timer expires, it rebroadcasts the RREQ. It attempts discovery up to a certain maximum number of times. If no route is discovered after the maximum number of attempts, the session is aborted.

3.2.2 Route Table Management

To manage the route table it will be needed for the useful information that is also stored in the route table entries and is called the soft-state associated with the entry.
Parameters associated with routing entry are:

- *Route request expiration timer:* is a timer associated with reverse path routing entries. The purpose of this timer is to purge reverse path routing entries from those nodes that do not lie on the path from the source to the destination
- *Route caching timeout:* is a time associated with routing entries. It indicates the time after which the route is considered to be invalid.

A neighbour is considered active, for that destination, if it originates or relays at least one packet for that destination within the most recent active timeout period.
Each time a route entry is used to transmit data from a source toward a destination, the timeout for the entry is reset to the current time plus *active route timeout*.

3.2.3 Path Maintenance

When a link break in an active route occurs, due to movement of one of the nodes lying on the active path, the node upstream of the break has to know that failure in sending data through this path to invalidate all its routes that utilized that link.
There are different mechanisms to detect the failure in active path as follow:

- Periodic hello messages can be used to ensure symmetric links as well as to detect link failures.
- By using link-layer acknowledgments (LLACKS).
- A link failure is also indicated if attempts to forward a packet to the next hop fail.

The node upstream of the break propagates a Route Error (RERR) packet, and places the IP address of each destination, which is now unreachable - due to the link break, in that packet. Whenever a node receives RERR it looks at the Routing Table and removes all the routes that contain the bad nodes. The node then broadcasts the RERR message to its neighbours.
When a neighbouring node receives the RERR, it in turn invalidates each of the routes listed in the packet, if that route used the source of the RERR as a next hop. If one or more routes are deleted, the node then creates and broadcasts its own RERR message. Once a source node receives the RERR, it invalidates the listed routes as previously described. If it determines that it still needs any of the expired routes, it then re-initiates route discovery for that route.

3.3 MIFA

MIFA [5] has been proposed in order to avoid the problems of MIP without needing to insert intermediate nodes between the FA and the HA. The basic idea of MIFA is that the HA delegates the authentication to the FA. As a result the FA authenticates the MN on behalf of the HA. Thus, the MN sends **Reg**istration **R**e**q**ue**st** (Reg_Rqst) to the FA, which in turn directly replies by sending a **Reg**istration **R**e**ply** message (Reg_Rply) to the MN. After receiving the Reg_Rply, the MN can resume transmission on uplink. In downlink a tunnel is established to forward the packets, arriving at the previous FA, to the new FA until the HA is informed about the movement and a tunnel from the HA to the current FA is established to forward the packets directly to the new FA. Thus the delay experienced from the communication between the new FA and the HA is hidden from the application, similar to micro mobility protocols. Additionally the time required to build an IPSec tunnel between the HA and the FA, if needed, is avoided too.

The local authentication by FAs relies on groups of neighboring FAs. Each FA defines a set of neighboring FAs called a **L**ayer**3-F**requent **H**andoff **R**egion (L3-FHR) [18]. These L3-FHRs can be built statically by means of standard algorithms (e.g. neighbor graph [11] or others [12]), or dynamically by the network itself, by observing the movements of the MNs. Typically, the L3-FHR of a FA consists of a small number of the FAs compared to the whole number of the FAs the MN may connect to. Every FA defines its own L3-FHR. The L3-FHR doesn't necessarily comprise all of the adjacent FAs, e.g. in the case of physical obstacles between the areas that prevent a movement between the adjacent FA areas.

In order to use MIFA, there must be a security association between the FAs in each L3-FHR.

IV- FAST INTER-CONNECTING BETWEEN WLAN AND AD HOC NETWORKS

The used network topology is illustrated in Figure 1-1. There are two Ad hoc networks. Each Ad hoc network is connected to a sub-network controlled by a certain FA. The wireless interfaces of APs are part of the Ad hoc network. To be able to secure the communication and the registration process a global AAA infrastructure is

required. An AAAH server is located in the home domain, whereas an AAAF exists in each foreign administrative domain.

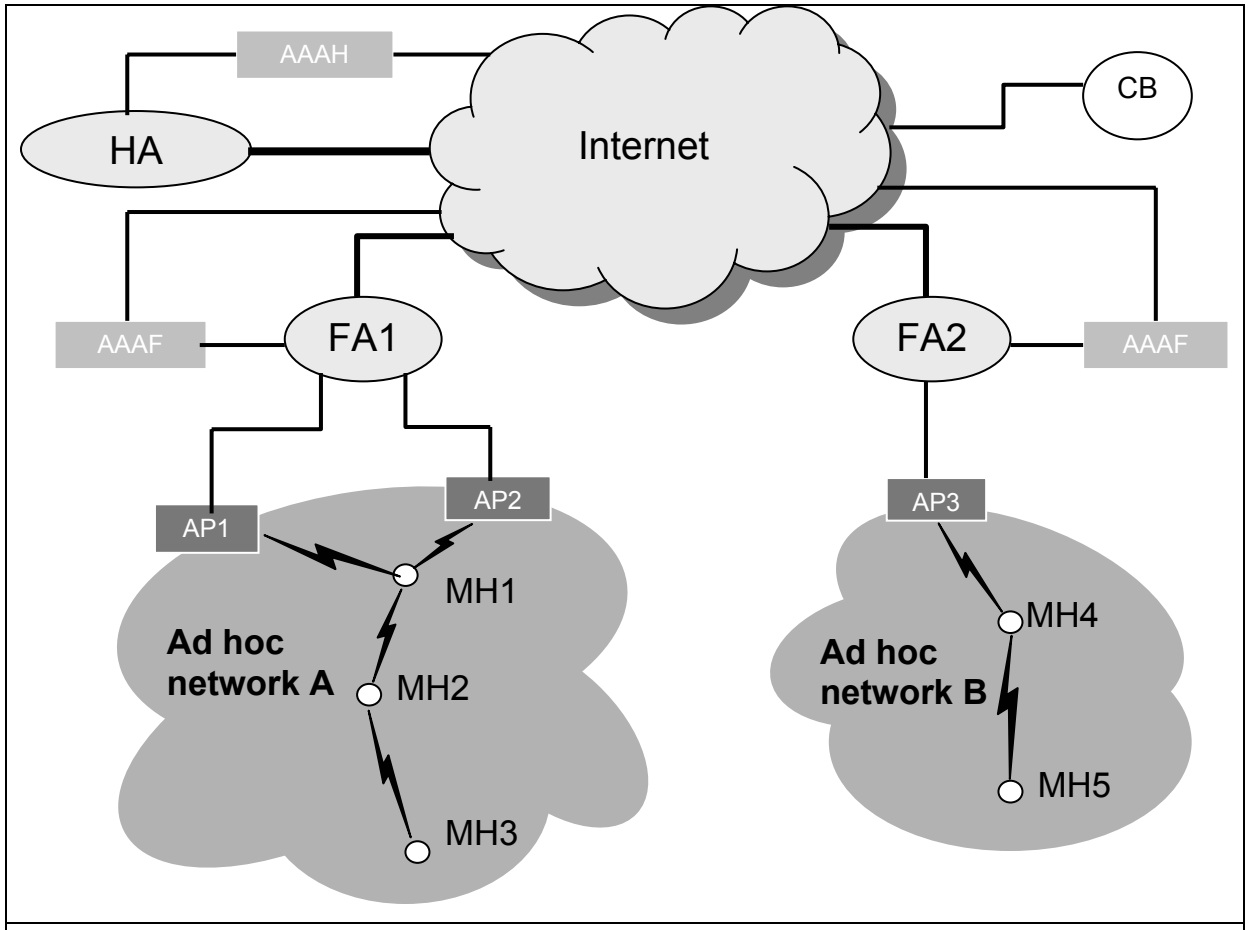

Figure 1: Network Topology

We have extended AODV by adding a new message called AODV connect request (***AODV_CON_REQ***) message. The extended AODV uses the fast authentication principle used in MIFA to support fast and smooth handoffs between the sub-networks and between the administrative domains. However, it does not need the L3-FHRs required by MIFA. We suppose that the MN3 goes inside the first Ad hoc network. MN1 and MN2 are members of the first Ad hoc network, while MN4 and MN5 locate in the second Ad hoc network. The Ad hoc networks are working on different channels.

a) Initial registration

When the MN3 is switched on or wants to connect to the Internet, at first it discovers the path to the FA and registers with it as depicted in figure 2. The MN broadcasts a ***RREQ*** with the advertisement extension, see [8]. Upon receiving of this message by an Ad hoc node, it checks if it has an entry to the FA. If this is the case, it sends a ***RREP*** with the ***Agent_Adv*** message of the FA. If the Ad hoc node has no entry to any FA it broadcasts the ***RREQ*** further.

As soon as the MN3 receives the ***RREP*** with the Advertisement, it sends an ***AODV_CON_REQ*** message along the discovered path to the certain FA. This message has to contain the fields of the registration message according to MIP.

The FA extracts the ***REG_REQ*** and encapsulates it in an **A**AA - **M**obile Node **R**equest message (AMR) and sends it to the controlling AAAF server. The AAAF server requests a FA-HA session key by including the suitable extensions defined in AAA protocols and sends the ***AMR*** message through the required proxies to the AAAH server. Upon receiving of the ***AMR*** by the AAAH, it generates a MN, FA session key (***K1***) and a MN, FA nonce. ***K1*** is used to authenticate the messages exchanged between the MN and the current FA. Another FA, HA nonce and session key (***K2***) to authenticate the messages exchanged between the current FA and the HA are generated by AAAH too. The new generated keys and nonces are added in suitable extensions to the ***AMR*** message, a **H**ome **A**gent MN **R**equest message (***HAR***) is built and sent to the HA. The HA extracts the FA, HA session key, FA, HA nonce and the ***Req_Rqst*** message encapsulated in the ***HAR*** message and processes it according to MIP procedures.

After that, the HA builds a ***REG_REP*** message, adds the nonces and the keys produced by the AAAH server to the message, encapsulates it in a **HA** MN **A**nswer message (***HAA***) and sends it to the AAAH server. An **A**AA - **M**obile Node **A**nswer message (***AMA***) is built then and forwards it to the AAAF server of the current FA's domain.

As soon as the AAAF server receives the ***AMA*** message, it generates two random variables ***R1***, ***R2*** which will be used for authentication purposes in the future registration, see [5]. Another Key is generated (***K3***) to authenticate the control messages between the MN and the next FA, the MN will move to. The new

generated keys and random variables are encapsulated within the received ***AMA*** message and forwarded to the current FA.

The current FA extracts then the ***Reg_Rply*** message, ***K1***, ***K2***, ***K3***, ***R1***, ***R2***, builds an ***AODV_CON_REP*** and sends it with ***K1***, ***K3***, ***R1*** and ***R2*** to the MN. After these procedures the MN is able to communicate with any node in the Internet.

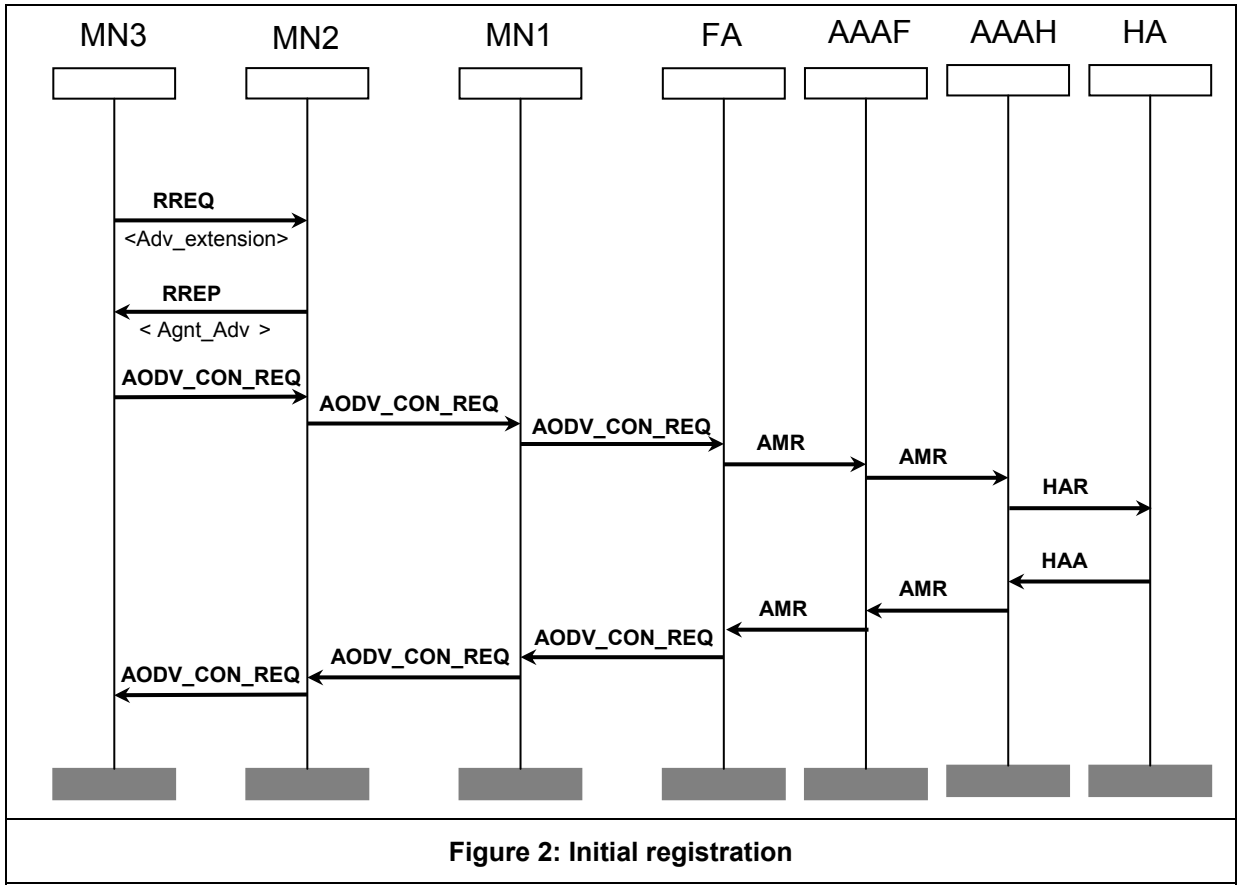

Figure 2: Initial registration

b) Moving inside the same Ad hoc network

When the MN3 moves inside the same Ad hoc network connected to the same FA, it uses the standard AODV to detect the new route.

c) Moving between two Ad hoc networks

Because of the high dynamics of Ad hoc networks, it is possible that the MN3 changes its route to the FA. The MN3 should achieve a layer3 handoff, it detects that it has to change the FA, that provides an access to the Internet for the MN3.

The MN has to detect the route to the new FA, therefore it broadcasts a ***RREQ*** with the advertisement extension. Upon receiving of ***RREP*** with the ***Agent_Adv*** message of the new FA, the MN3 builds and sends an ***AODV_CON_REQ*** message to the new FA. This message contains the fields of ***REG_REQ*** message. However, ***REG_REQ*** is built here according to MIFA procedures.

When the new FA receives this message, it detects that the MN3 tries to use MIFA to accelerate the handoff. Therefore, it extracts the ***REG_REQ***, builds and sends an ***AMR*** message to the AAAF responsible for it (AAAF2 in the figure). AAAF2 sends this message to the AAAF server of the old FA (AAAF1 in the figure). The new FA asks the AAA infrastructure in this message to build a security association between itself and the old FA. AAAF1 extracts the ***REG_REQ*** and builds a security association (***K4***) between the old and the new FA.

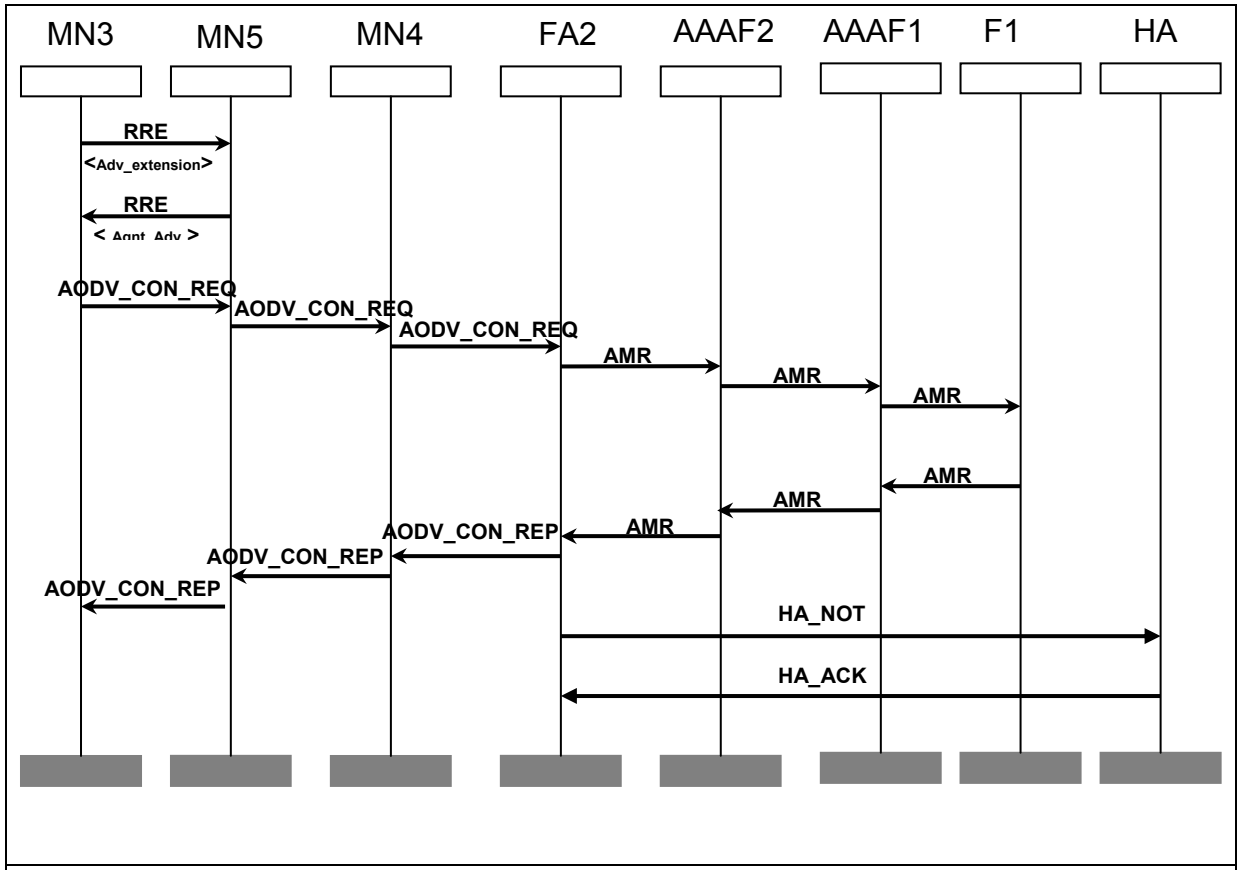

Figure 3: Movement between two Ad hoc networks

REG_REQ message and the key (***K4***) are sent to the old FA, which processes the message according to MIFA procedure. A ***REG_REP*** message is built and sent with the ***M_P_Not*** to the AAAF1, which sends them with the key ***K4*** to the AAAF2. The

data existing in ***M_P_Not*** message is encrypted using ***K4***. AAAF2 builds then an ***AMA*** message and sends it to the AAAF2, which forwards them to the new FA with two new generated random variables ***R1new***, ***R2new*** and a new key ***K5***. ***K5*** is used to authenticate the registration with the next FA to which the MN will move, while ***R1new***, ***R2new*** are used for authentication purposes. The FA extracts the ***REG_REP***, builds an ***AODV_CON_REP*** and forwards it to the MN3 with the new generated random variables and ***K5***. Additionally, the new FA extracts the ***K4***. After that, it decrypts the information existing in the ***M_P_Not*** and informs the HA by sending a ***HA_Not*** that it has to tunnel the packets, sent to the MN, to the new binding. The HA responds by sending a ***HA_Ack*** containing the information required for the next registration according to MIFA.

V- CONCLUSION

In this paper, we have proposed and described a seamless handoff solution, which enables the connecting between WLAN and Ad hoc networks. We have extended AODV by adding two new messages, which are AODV_CON_REQ and AODV_CON_REP. These messages carry the fields of REG_REQ and REG_REP. The fast authentication used in MIFA is used here in the registration too. However, we do not need any L3-FHR as is the case by MIFA.

Our proposal should minimize the handoff latency and outperform the other interconnecting approaches proposed in the literature. This is because of the elimination of the impact of the delay between the HA and the FA on the performance. A key issue is that our approach does not require any hierarchy such as the other approaches do.

Currently, we develop a mathematical model to evaluate the performance compared to other proposals. We are now simulating the introduced approaches with ns-2 [13] to study the performance using TCP traffic.

References:

[1]. M. S. Gast. : 802.11 Wireless Networks. The Definite Guide, O'Reilly, 2002.
[2] S.Basagni, M.Conti, S.Giordano, I.Stojmenovic : Mobile Ad Hoc Networking. Institute of Electrical and Electronics Engineers, Inc. ISBN 0-471-37313-3, 2004.
[3] C.Perkins: Mobile IP. IEEE Communications Magazine, 66-82, May 2002.
[4] C.Perkins, E. Belding-Royer: Ad hoc On Demand Distance Vector Routing. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[5] A. Diab, A. Mitschele-Thiel: Minimizing Mobile IP Handoff Latenc. 2nd International Working Conference on Performance modelling and Evaluation of Heterogeneous Networks (HET-NETs'04), Ilkley, West Yorkshire, U.K., July 2004.
[6] C. Åhlund1, A. Zaslavsky2: Software Solutions to Internet Connectivity in Mobile Ad Hoc Networks
[7] T. ville: Micro-Mobility wireless Ad hoc networks, towards hybrid wireless Multi hop networks.
Department of Electrical Engineering University of Oula,Oula, Finland. Diploma thesis, 2001.
[8] Y. Sun, E. M. Belding-Royer, C. E. Perkins : Internet Connectivity for
Ad hoc Mobile Networks. International Journal of Wireless Information Networks special issue on 'Mobile Ad Hoc Networks (MANETs): Standards, research, Applications', vol. 9, no. 2, pp. 75-88, Apr, 2002.
[9] C. Åhlund: Extended Mobile IP and support for Global Connectivity in Hybrid Networks. Department of Computer Science and Electrical Engineering Luleå University of Technology Luleå Sweden, SE-971 87, January 2005.
[10] P. Ratanchandani, R. Kravets : A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks.
Wireless Communications and Networking, pp. 1522-1527, Mar. 2003.
[Ref-ns-2] Network simulator ns-2, URL: http://www.isi.edu/nsnam/ns/
[11]S. Pack, Y. Choi: Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN. Networks 2002, August 2002.
[12]S.K. Sen, et al.: A Selective Location Update Strategy for PCS Users. ACM/Baltzer J. Wireless Networks, September 1999.
[13] Network simulator ns-2, URL: http://www.isi.edu/nsnam/ns/

Authors:

Dipl.-Ing. Ausama Yousef
Prof. Dr.-Ing. habil. Andreas Mitschele-Thiel
Dipl.-Ing. René Boeringer
Dipl.-Ing. Ali Diab
TU Ilmenau, Gustav-Kirchhoff-Str. 1
D-98693 Ilmenau
Phone: +49 (0)3677 69 1338
Fax: +49 (0)3677 69 1220
E-mail: ausama.yousef@tu-ilmenau.de